Amendments to the Specification:

*Please amend the specification at page 1, paragraph [0001] as follows:

[0001] The present application claims the benefit of U.S. Provisional Patent Application Nos. 60/418,762, filed October 15, 2002 and 60/421,254, filed October 25, 2002. The present application is also a continuation in part of U.S. Patent Application No. 10/275,197, filed March 4, 2003 (published as US 2004-0128512 A1), which is the national stage of International Application No. PCT/US01/14014, filed April 30, 2001 (published in English as WO 01/84438 A1). The present invention is also a continuation in part of U.S. Patent Application No. 10/370,421, filed February 19, 2003 (published as US 2004-0049401 A1), which claims the benefit of U.S. Provisional Patent Application No. 60/358,321, filed February 19, 2002. The present application is also a continuation in part of U.S. Patent Application No. 10/394,507, filed March 21, 2003 (published as US 2004-0047490), which claims the benefit of U.S. Provisional Patent Application No. 60/367,033. The present application is also related to assignee's U.S. Patent Application No. 09/938,870, filed August 23, 2001 (published as US 2002-0099943 A1) and assignee's concurrently filed U.S. Patent Application No. 10/686,495, titled "Identification Document and Related Methods," (published as US 2004-0181671 A1). ~~(attorney docket P0895 – inventors Trent Brundage, et al.).~~ Each of these patent documents is herein incorporated by reference.

*Please amend the specification at paragraph [0044], spanning pages 11-12, as follows:

[0044] One aspect of the present invention utilizes a digitally watermarked document 10 in an online (e.g., internet or other network) voting system. Registered voters receive a digitally watermarked ballot (or other watermarked document). The ballot preferably includes an embedded voting identifier that helps to facilitate access to a voting website or other network interface. In one embodiment, the identifier is used to link to an appropriate voting web site. For example, the identifier, once decoded from a watermark,

is provided to a database to index a corresponding URL or IP address stored in a database. Further information regarding watermark-based linking is found, e.g., in assignee's U.S. Patent Application No. 09/571,422, filed May 15, 2000 (now U.S. Patent No. 6,947,571), which is herein incorporated by reference. In another embodiment, a watermark identifier provides an additional security feature or verifies an ability to vote. For example, verifying an ability to vote may include identifying an eligible voter, verifying voter eligibility, identifying a registered voter, verifying residency or citizenship, anonymously identifying a voter, pointing to a voter identifier or account, etc. In a preferred voting embodiment, a voter must have physical possession of the watermarked ballot (or other voter document) to be able to vote. In this voting embodiment, the ballot is presented to a watermark reader, which extracts an embedded identifier, and passes the extracted identifier to a central or distributed voting server. The identifier can be compared against a list or range of valid identifiers.). Of course, a watermarked ballot can be used in combination with other security features, such as a password or PIN. In this case, a voter demonstrates both physical possession of a watermark ballot (or other document), and knowledge of a password or PIN.

*Please amend the specification at paragraph [0053], spanning pages 14-15, as follows:

[0053] In a related implementation we steganographically embed characteristics associated with a cardholder's biometric features, e.g., fingerprint, facial recognition, DNA-print, etc., in an identification document 10 or other card. The characteristics may even include a hash of such biometric information. The term "hash" is broadly used in this document to include a reduced representation of a value, text or template. To verify that a person is not just, e.g., using their older sister's identification document for an online transaction, the cardholder must present her watermarked document, which includes an embedded age indicator and embedded biometric characteristic, as well as a fresh biometric sample (e.g., her fingerprint). If the biometric sample and the embedded sample match, and if the embedded age indicator is sufficient for the activity, the activity or transaction can proceed. Similar techniques can be used to verify age at a bar, casino,

or for the purchase of age-limited goods or merchandise – all without compromising the person's identity. Steganographically embedding biometric information is discussed even further, e.g., in assignee's U.S. Patent Application No. 10/366,541 (now U.S. Patent No. 6,804,378), which is a continuation of U.S. Patent No. 6,546,112, and in U.S. Provisional Patent Application No. 60/493,687, filed August 7, 2003. Each of these patent documents is herein incorporated by reference.

*Please amend the specification at paragraph [0071] on page 20 as follows:

[0071] The following section relates to U.S. Patent Application Nos. 10/319,404 (published as US 2003-0149879 A1); 10/319,380 (published as US 2003-0179900 A1); 10/435,517 (now U.S. Patent No. 7,006,662); and 10/435,612 (published as US 2004-0044894 A1). Each of these patent documents is herein incorporated by reference.